



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/598,832	09/13/2006	Dimitri Korobkov	73408.8001.US00	1975
70416	7590	07/08/2011	EXAMINER	
Perkins Coie LLP			SU, SARAH	
Patent - LA			ART UNIT	PAPER NUMBER
P.O. Box 1208			2431	
Seattle, WA 98111-1208			NOTIFICATION DATE	DELIVERY MODE
			07/08/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentprocurement@perkinscoie.com

Office Action Summary	Application No.	Applicant(s)	
	10/598,832	KOROBKOV, DIMITRI	
	Examiner	Art Unit	
	SARAH SU	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 08 June 2011.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-5, 9-17 and 21-25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-5, 9-17, 21-25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8 June 2011 has been entered. In this amendment, claims 1, 10, and 13 have been amended, and claim 30 has been cancelled.
2. Claims 1-5, 9-17, and 21-25 are presented for examination.

Response to Arguments

3. With regards to the objection to the claims, the applicant has submitted claim amendments, and the examiner hereby withdraws the objections.
4. Applicant's arguments filed 8 June 2011 have been fully considered but they are not persuasive.

As to claim 1, it is argued by the applicant that Shefi does not disclose providing a first random generator on the communication device which determines addresses on the digital storage medium. The examiner respectfully disagrees. Shefi discloses that random numbers are generated to form at least a portion of a key which is substantially identical to a pointer (i.e. address), which points to a location of an obtained random number in a table (col. 4, lines 40-51, 58-62).

Further, it is argued by the applicant that Shefi addresses a different technical problem than the present patent application. It has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, Shefi is also related to the field of using a one time pad to secure communications. It is also noted that the applicant argues that Shefi removes the need for "physical one-time pads", wherein the claimed invention addresses the technical problem of using "physical one-time pads" more efficiently. If the applicant's claims (i.e. storage of symbols on digital storage medium) are to be interpreted as using "physical one-time pads" more efficiently, then Shefi can also be considered to disclose "physical one-time pads" since Shefi also discloses the storage of random numbers on memory (col. 4, lines 10-17). Bush also discloses that one time pads may be stored on memory chips (Abstract, lines 11-13).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2431

6. Claims 1, 2, 4, 5, 11-14, 16, 17, 24, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bush (US 2002/0002675 A1) in view of Shefi (US 6,445,794 B1).

As to claim 1, Bush discloses a system and method for secure encryption of data packets for transmission over unsecured networks, the system and method having:

providing a communication device which has an interface for a digital storage medium, whose content may be read out and duplicated (0032, lines 3-5),

providing the digital storage medium which is connected to the interface, storing a supply of symbols for encryption on the digital storage medium (0032, lines 3-5; 0061, lines 1-6);

reading out the symbols from the digital storage medium using the addresses on the digital storage medium (0032, lines 3-5; 0061, lines 1-6),

employing the read out symbols for encrypting or decrypting the digital data stream of the communication device (0041, lines 4-9; 0042, lines 3-12).

Bush fails to specifically disclose:

providing a first random generator on the communication device which determines addresses on the digital storage medium.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Bush, as taught by Shefi.

Art Unit: 2431

Shefi discloses a system and method for synchronizing one time pad encryption keys, the system and method having:

providing a first random generator on the communication device which determines addresses (i.e. pointer) on the digital storage medium (i.e. non-volatile memory) (col. 4, lines 40-51, 58-62).

Given the teaching of Shefi, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Bush with the teachings of Shefi by randomly determining an address of symbols on a storage medium. Shefi recites motivation by disclosing that randomly selecting symbols to be used for encryption/decryption produces a system that uses a one-time pad that can be used for secure communication on an insecure channel or for secure identification which is automated and practicable for wide-spread communication while not being liable to a brute force attack on the one-time pad itself (col. 3, lines 65-67; col. 4, lines 1-4). It is obvious that the teachings of Shefi would have improved the teachings of Bush by randomizing which symbols are selected for encryption by randomly generating addresses in order to provide for secure communication using a one-time pad while protecting against brute force attacks on the one-time pad.

As to claim 13, Bush discloses:

an interface for a replaceable or writable storage medium, whose content may be read out and duplicated, the storage medium connected to the interface comprising a supply of symbols for encryption, which may be

Art Unit: 2431

read by using an address or storage on the storage medium (0032, lines 3-5; 0061, lines 1-6),

an encryption unit, which is set up so that it uses the supply of symbols for encrypting or decrypting the digital data stream of the communication devices by accessing this supply through the addresses (0041, lines 4-9; 0042, lines 3-12).

Bush fails to specifically disclose:

a first random generator on the communication device which determines the address on the storage medium.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Bush, as taught by Shefi.

Shefi discloses:

a first random generator on the communication device which determines the address (i.e. pointer) on the storage medium (i.e. non-volatile memory) (col. 4, lines 40-51, 58-62).

Given the teaching of Shefi, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Bush with the teachings of Shefi by randomly determining an address.

Please refer to the motivation recited above with respect to claim 1 as to why it is obvious to apply the teachings of Shefi to the teachings of Bush.

As to claims 2 and 14, Bush discloses:

Art Unit: 2431

wherein the symbols on the storage medium are only used once

(0013, lines 8-10).

As to claims 4 and 16, Bush discloses:

wherein the communication device is a radio device, laptop, PDA, or

a mobile telephone which has an interface for a memory card (0013, lines 12-15).

As to claims 5 and 17, Bush discloses:

wherein the storage medium is a flash memory card, a hard drive, or

an optical storage drive, whose information may be addressed (0013, lines 17-18).

As to claims 11 and 24, Bush discloses:

wherein a permutation of the digital data stream is performed before

it is transmitted (0044, lines 4-6).

As to claims 12 and 25, Bush fails to specifically disclose:

wherein the symbols on the storage medium are generated by the

noise of an analog source using an A/D converter.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Bush, as taught by Shefi.

Art Unit: 2431

Shefi discloses a system and method for synchronizing one time pad encryption keys, the system and method having:

wherein the symbols on the storage medium are generated by the noise of an analog source using an A/D converter (col. 4, lines 58-64) but does not disclose the usage of an A/D converter.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use an A/D converter to convert an analog signal to a digital signal since it was known in the art that an analog noise signal must be converted before it can be used in a digital system.

Given the teaching of Shefi, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Bush with the teachings of Shefi by using an analog noise source.

Shefi recites motivation by disclosing that using a source of physical random phenomena can produce true random numbers (col. 4, lines 58-60). It is obvious that the teachings of Shefi would have improved the teachings of Bush by using an analog noise source in order to produce true random numbers.

7. Claims 3, 9, 15, 21, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bush in view of Shefi as applied to claims 1 and 13 above, and further in view of Kauffman et al. (US 2002/0159588 A1 and Kauffman hereinafter).

As to claims 3 and 15, Bush in view of Shefi fails to specifically disclose:

wherein the symbols are encrypted and decrypted with the data stream using mod2.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Bush in view of Shefi, as taught by Kauffman. Kauffman discloses a system and method for cryptography with unconditional security, the system and method having:

wherein the symbols are encrypted and decrypted with the data stream using mod2 (0004, lines 1-9).

Given the teaching of Kauffman, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Bush in view of Shefi with the teachings of Kauffman by using mod2 for encryption and decryption. Kauffman recites motivation by disclosing that using modulo 2 for encryption reduces the data size of the resulting cryptogram (0004, lines 1-3). It is obvious that the teachings of Kauffman would have improved the teachings of Bush in view of Shefi by using mod2 for encryption and decryption in order to produce a cryptogram that is smaller in size.

As to claims 9 and 21, Bush in view of Shefi fails to specifically disclose:

wherein a status of the first random generator is transmitted to synchronize the encryption.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Bush in view of Shefi, as taught by Kauffman.

Art Unit: 2431

Kauffman discloses:

**wherein a status of the first random generator is transmitted to
synchronize the encryption** (0031, lines 10-15).

Given the teaching of Kauffman, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Bush in view of Shefi with the teachings of Kauffman by transmitting the status of a generator for synchronization. Kauffman recites motivation by disclosing that the receiver must have the same random number sequence the sender used or must be able to reproduce it in order to perform successful encryption and decryption (0005, lines 3-5). It is obvious that the teachings of Kauffman would have improved the teachings of Bush in view of Shefi by transmitting information for synchronizing the symbols in order to ensure that the sender and receiver are using the same sequence.

As to claim 22, Bush in view of Shefi fails to specifically disclose:

**means, through which the status of the first random generator is
transmitted at specific intervals.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Bush in view of Shefi, as taught by Kauffman.

Kauffman discloses:

**means, through which the status of the first random generator is
transmitted at specific intervals** (0021, lines 11-15).

Art Unit: 2431

Given the teaching of Kauffman, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Bush in view of Shefi with the teachings of Kauffman by transmitting the status of a generator at specific intervals. Kauffman recites motivation by disclosing that synchronizing at regular intervals thwarts attackers from attacking the random generator's state (0021, lines 13-14) while ensuring that the sender and receiver are using the same sequence (0005, lines 3-5). It is obvious that the teachings of Kauffman would have improved the teachings of Bush in view of Shefi by transmitting synchronization information at specific intervals in order to prevent attackers from attacking a generator's state while ensuring that successful encryption and decryption can be performed.

8. Claims 10 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bush in view of Shefi as applied to claims 1 and 13 above, and further in view of Glover (US 6,868,495 B1).

As to claims 10 and 23, Bush in view of Shefi fails to specifically disclose:

**wherein there is a second random generator which performs
scrambling of access to individual segments on the storage medium if the
first random generator determines concrete addresses of the segments.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Bush in view of Shefi, as taught by Glover.

Art Unit: 2431

Glover discloses a system and method for one-time pad encryption key distribution, the system and method having:

wherein there is a second random generator which performs scrambling of access to individual segments on the storage medium if the first random generator determines concrete addresses of the segments
(col. 22, lines 51-56).

Given the teaching of Glover, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Bush in view of Shefi with the teachings of Glover by scrambling access to symbols. Glover recites motivation by disclosing that changing parameters and decrypting code helps to thwart the efforts of a brute force attack (col. 22, lines 66-67; col. 23, line 1). It is obvious that the teachings of Glover would have improved the teachings of Bush in view of Shefi by scrambling access to symbols in order to prevent brute force attacks.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SARAH SU whose telephone number is (571)270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

Art Unit: 2431

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/NATHAN FLYNN/
Supervisory Patent Examiner, Art Unit 2431

/Sarah Su/
Examiner, Art Unit 2431